STEGANOGRAFI MENGGUNAKAN METODE *DISCRETE FOURIER TRANSFORM* (DFT)

Yuri Ariyanto[1], Rizky Ardiansyah[2], Bias Paris[3]

[1,2]Program Studi Teknik Informatika, Jurusan Teknologi Informasi, [3]Politeknik Negeri Malang
[1]yuri@polinema.ac.id, [2]risky.computerscience@gmail.com, [3]bias.riot@gmail.com

Abstrak

Seiring dengan kemajuan teknologi, serangan terjadi pada industri *photography* di mana banyak penyalahgunaan foto yang memiliki hak cipta tanpa seijin pemilik foto tersebut. Karena itulah dibuat sebuah aplikasi yang berfungsi untuk menyisipkan *watermark* dengan menggunakan metode DFT (*Discrete Fourier Transform*). Metode tersebut adalah metode matematika yang sering digunakan dalam bidang elektronika dan komputer. Metode ini secara khusus digunakan untuk menyelesaikan masalah yang berhubungan dengan frekuensi, sehingga metode ini dapat digunakan dalam bidang citra *digital*. Metode ini diterapkan untuk melakukan penyisipan dan ekstraksi *watermark* pada citra penampung. *Watermark* tersebut disisipkan kedalam frekuensi domain pada gambar dan akan menghasilkan *output* citra ber-*watermark* atau *embeded image*. Hal ini adalah untuk mencegah penyalahgunaan hak cipta, namun *watermark* tersebut tidak nampak secara fisik. Hal ini dilakukan selain memberikan jaminan keamanan terhadap gambar, tapi juga tidak mengurangi estetika pada gambar tersebut. Analisa yang dilakukan adalah tingkat keberhasilan proses *insertion* dan *extraction*, serangan pada citra, uji kemiripan dengan pengujian NPCR (*Number of Pixel of Change Rate*), UACI (*Unified Averaged Changed Intensity*), dan PSNR (*Peak Signal-to-Noise Ratio*) pada proses *insertion* dan *extraction*. DFT disimpulkan aman terhadap serangan berupa *cropping*, *resize*, dan *editing*. Selain itu, dihasilkan nilai presentase perubahan yang rendah pada pengujian NPCR & UACI dan nilai yang tinggi pada pengujian PSNR.

Kata kunci : Discrete Fourier Transform, Watermark, embeded image, photography, frekwensi

1. Pendahuluan

Kemajuan teknologi saat ini telah mampu merubah banyak sekali kehidupan dan kebiasaan aktifitas manusia. Salah satunya kini manusia dapat saling bertukar dan mengirim informasi dengan sangat cepat dan mudah tanpa mengenal jarak dan waktu. Sehingga banyak hal-hal baru yang muncul baik jual beli, bersosial, trend, bisnis, dan banyak lagi. Seiring dengan hal itu maka kebutuhan akan keamanan komputer semakin dibutuhkan, untuk melakukan pecegahan terhadap serangan-serangan dari peretas.

Para peretas bisa melakukan berbagai macam hal termasuk penyadapan informasi yang bisa sangat merugikan bagi korbanya, sehingga banyak sekali berbagai macam upaya untuk melakukan mencegahan berbagai macam serangan peretas, diantaranya adalah kriptografi.

Namun walaupun telah ada kriptografi, bukan berarti data yang di simpan menjadi 100% aman. Karena namun peretas juga bisa menemukan celah untuk membuka atau memecahkan enkripsi yang telah dibuat untuk mndapatkan informasi.

Maka dengan berbagi hal yang telah terjadi, munculah sebuah metode yang bisa di bilang lebih aman di banding kriptografi, yang sering disebut dengan steganografi. Didalam steganografi, kita bisa menyembunyakan sebuah pesan, gambar, maumpun file kedalam sebuah gambar, video, maupun audio. Didalm steganografi, terdapat proses penyisipan bit-bit pesan kedalam bit-bit penampung pada tiap-tiap pixel citra. Sehingga penampung/citra yang telah di sisipi pesan bisa di kirimkan tanpa menimbulkan kecurigaan, Karena dalam metode ini mata dan telinga manusia tidak dapat melihat dan mendengar suatu perubahan yang sangat kecil akibat penyisipan pesan yang dilakukan lakukan melalui steganografi.

Steganografi juga berkembang menjadi digital watermarking, dan sangat berguna dalam bidang *photography*. Fotografer seringkali menjumpai tindakan-tindakan yang tidak diinginkan yang berkaitan pencurian foto hasil foto mereka, sehingga timbulah perkembangan dari steganografi yang diterapkan kedalam bidang *photography*. Dalam kasus saat ini *"Inod Photography"* sebagai salah satu komunitas *photography* yang ingin menerapkan steganografi atau *digital*

watermarking kedalam hasil foto komunitas tersebut. Harapan komunitas tersebut, bahwa hasil foto-foto kamunitas tidak mudah untuk di klaim oleh pihak lain.

1.1 Rumusan Masalah

Berdasarkan latar belakang di atas maka bisa disimpulkan beberapa masalah berikut:

1. Apakah penerapan metode DFT tepat untuk menyelesaikan permasalahan di inod photography?
2. Apakah penggunaan metode DFT tahan terhadap serangan cropping, rotasi, dan filtering pada *embedded image*?

1.2 Batasan Masalah

Batasan masalah yang diangkat dalam skripsi ini dapat dipaparkan sebagai berikut:

1. Aplikasi yang dibangun menggunakan algoritma DFT untuk melakukan *insertion* dan *extraction.*
2. Format file citra penampung dan *watermark* yang digunakan adalah jpg.
3. Citra penampung yang digunakan adalah citra berwarna (RGB), sedangkan citra *watermark* berwarna *monochrome*.
4. Citra *watermark* yang digunakan adalah citra berukuran 50x50 dan tidak dapat diubah
5. Ukuran citra penampung minimal 100x100 pixel

1.3 Tujuan

Tujuan yang ingin dicapai dalam penelitan ini adalah:

1. Menyelesaikan masalah di *inod photograpy*
2. Membuat aplikasi steganografi dengan menggunakan metode DFT

2. Tinjauan Pustaka

2.1 *Discrete Fourier Transform*

DFT merupakan prosedur matematika yang digunakan untuk menentukan harmonik atau frekuensi yang merupakan isi dari urutan sinyal diskrit. Urutan sinyal diskrit adalah urutan nilai yang diperoleh dari sampling periodik sinyal kontinu dalam domain waktu [4]. DFT berasal dari fungsi Transformasi Fourier X(f) yang didefinisikan:

$$\boldsymbol{X(f) = \int_{\infty}^{\infty} x[t].e^{-f2\pi ft}dt} \quad (1)$$

Dimana:

N = jumlah sampel input
X(m) = urutan ke-m komponen output DFT(X(0), X(1),…,X(N-1))
m = indeks output DFT dalam domain frekwensi (0,1,…,N-1)
x(n) = urutan ke-n sampel input (x(0),x(1),…,x(N-1))
n = indeks sampel input dalam domain waktu (0,1,…,N-1)
j = bilangan imajiner ($\sqrt{-1}$)
π = derajat (180^o)
e = logaritma natural (2.718281828459)

Dalam bidang pemrosesan sinyal kontinu, Persamaan 1 digunakan untuk mengubah fungsi domain waktu kontinu x(t) menjadi fungsi domain frekuensi kontinu X(f). Fungsi X(f) memungkinkan untuk menentukan kandungan isi frekuensi dari beberapa sinyal dan menjadikan beragam analisis sinyal dan pengolahan yang dipakai di bidang teknik dan fisika. Dengan munculnya komputer digital, ilmuwan di bidang pengolahan digital berhasil mendefenisikan DFT sebagai urutan sinyal diskrit domain frekuensi X(m), dimana:

$$\boldsymbol{f(x) = \sum_{n=0}^{N-1} x\,(n).e^{-f2\pi nm/N}} \quad (2)$$

Dimana:

N = jumlah sampel input
X(m) = urutan ke-m komponen output DFT(X(0), X(1),…,X(N-1))
m = indeks output DFT dalam domain frekwensi (0,1,…,N-1)
x(n) = urutan ke-n sampel input (x(0),x(1),…,x(N-1))
n = indeks sampel input dalam domain waktu (0,1,…,N-1)
j = bilangan imajiner ($\sqrt{-1}$)
π = derajat (180^o)

Kemudian hubungkan dengan rumus Euler $\boldsymbol{e^{-j0} = \cos(0) - j\sin(0)}$ sehingga setara dengan:

$$\boldsymbol{X(m) = \sum_{n=0}^{N-1} x\,(n).[cos\left(\frac{2\pi nm}{N}\right) - j\,sin\,(\frac{2\pi nm}{N})]} \quad (3)$$

Dimana:

N = jumlah sampel input
X(m) = urutan ke-m komponen output DFT(X(0), X(1),…,X(N-1))
m = indeks output DFT dalam domain frekwensi (0,1,…,N-1)
x(n) = urutan ke-n sampel input (x(0),x(1),…,x(N-1))
n = indeks sampel input dalam domain waktu (0,1,…,N-1)
j = bilangan imajiner ($\sqrt{-1}$)
π = derajat (180^o)

Meski lebih rumit daripada Persamaan 2, Persamaan 3 lebih mudah untuk dipahami. Konstanta j = √−1 hanya membantu membandingkan hubungan fase di dalam berbagai komponen sinusoidal dari sinyal. Nilai N merupakan parameter penting karena menentukan berapa banyak sampel masukan yang diperlukan, hasil domain frekuensi dan jumlah waktu proses yang diperlukan untuk menghitung N-titik DFT. Diperlukan N-perkalian kompleks dan N-1 sebagai tambahan. Kemudian, setiap

perkalian membutuhkan N-perkalian riil, sehingga untuk menghitung seluruh nilai N (X(0), X(1), …, X(N-1)) memerlukan N2 perkalian. Hal ini menyebabkan perhitungan DFT memakan waktu yang lama jika jumlah sampel yang akan diproses dalam jumlah besar.

Transformasi Fourier Diskrit (DFT) 2 Dimensi adalah tranformasi fourier diskrit yang dikenakan pada fungsi 2D (fungsi dengan dua variabel bebas), yang didefinisikan sebagai berikut :

$$F(u,v) = \frac{1}{MN}\sum_{y=0}^{M-1}\sum_{y=0}^{N-1} f(y,x)\left(\begin{array}{c} cos\left(2\pi\left(\frac{ux}{N}+\frac{vy}{M}\right)\right) \\ -j\,sin\left(2\pi\left(\frac{ux}{N}+\frac{vy}{M}\right)\right)\end{array}\right)$$

(4)

DFT 2D ini banyak digunakan dalam pengolahan citra digital, karena data citra dinyatakan sebagai fungsi 2D.

3. Hasil Penelitian dan Pembahasan

3.1 Metode Pengembangan

Bab ini menjelaskan langkah – langkah yang dilakukan untuk membuat Aplikasi yang mengimplementasikan steganografi dengan menggunakan metode *Discrete Fourier Transform (DCT)*

Langkah-langkah yang diperlukan antara lain:

1. Study Literatur

Pada tahap ini penelitian dilakukan dengan mempelajari berbagai literature melalui pengumpulan dokumen-dokumen, referesi buku, sumber-sumber dari internet, atau sumber-sumber lain yang diperluan untuk merancang dan mengimplementasikan system yang berkaitan dengan penulisan skripsi yang dilakukan.

2. Analisa Kebutuhan

Tujuan menganalisa antara lain menganalisa kebutuhan dan keperluan dasar yang akan digunakan dalam pembuatan aplikasi yang diinginkan. Hasil perancangan yang diperoleh adalah pembuatan aplikasi yang dapat melakukan steganografi dengan menggunakan metode *Discrete Fourier Transform (DFT).*

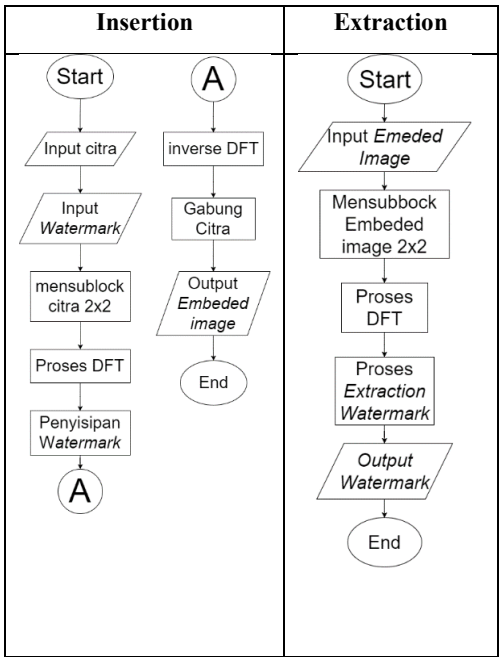
Algoritma penyisipan:

Dalam metode ini semua penyisipan dilakukan pada *frequency domain* dan diterapkan pada *source image*. Untuk mengkonversi dari *spatial domain* ke *frequency domain* masing-masing pixel (6 bit) di *spatial domain* di ubah menjadi dua bagian, bagian pertama *real* dan bagian lainya adalah *imaginary*. Bit watermark dimasukkan ke dalam bagian *real* frekuensi domain dari source image, tiap pixel dimasukan kedalam block pixel dengan ukuran 6x6 pixel per block pada source image. Proses ini diulang pada seluruh matriks gambar dengan cara yang sama. Maka proses selesai dilakukan DFT (2017).

Algoritma Ekstraksi:

Selama *decoding*, *embedded image* telah diambil sebagai *imput* pada *spatial domain*. Terapkan algoritma ekstraksi untuk mengekstrak pesan atau gambar otentikasi dari gambar stego. Proses ini diulang pada keseluruhan matriks *embedded image* dengan cara yang sama DFT (2017).

Tabel 1. Proses Sistem Secara Garis Besar



4. Implementasi

Implementasi steganografi dengan menggunakan metode *Discrete Fourier Transform (DFT)* mengacu kepada perancangan sistem. Langkah – langkah pada tahap implementasi dengan :

- Pembuatan scipt berdasarkan perancangan yang telah dibuat.
- Menggunakan bahasa pemrograman C#.
- Data yang digunakan ada 2 macam, pertama adalah foto yang akan di distribusikan olah "Inod Photography", dan yang kedua adalah watermark inod photography yang akan disisipkan

Tabel 2. Contoh Foto Dan Watermark Yang Akan Digunakan

Contoh foto yang akan di distribusikan	Contoh watermark
	

5. Pengujian dan Analisa

Pengujian dilakukan untuk menjamin dan memastikan bahwa sistem yang dirancang dapat

berjalan seperti yang diharapkan. Strategi pengujian perangkat lunak yang digunakan yaitu:

1. Pengujian Visual

Pengujian Visual digunakan untuk melihat kecocokan citra antara citra asli, citra terenkripsi, dan citra terdekripsi. Antara citra Asli dan citra terenkripsi diharuskan memiliki perbedaan yang besar, sedangkan citra asli dan citra terdekripsi diharuskan memiliki persamaan yang besar. Perhitungan untuk perbedaan hasil menggunakan rumus *Number of Pixel Change Rate (NPCR), y*ang mengindikasikan perbedaan pixel diantara dua citra. Dan rumus selanjutnya adalah *Unified Average Changing Intensity(UACI*), yang digunakan untuk rata-rata intensitas perbedaan pixel dari dua citra. Dan berikut adalah rumus matematika dari NPCR dan UACI:

$$\boldsymbol{NPCR} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \boldsymbol{D(i,j)}}{\boldsymbol{M\ x\ N}} \boldsymbol{x}\ \mathbf{100\%}$$

$$\boldsymbol{with: D(i,j) = 0\ if\ Io(i,j) = Ienc(i,j), 1}$$

$$\boldsymbol{UACI} = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\boldsymbol{|Io(i,j) - Ienc(i,j)|}}{\mathbf{25\ 5}} \right] \boldsymbol{x}\ \frac{\mathbf{100\%}}{\boldsymbol{M\ x\ N}} \quad (5)$$

Hasil yang diinginkan dari perhitungan NPCR adalah setinggi mungkin, sedangkan hasil dari UACI berada disekitar 33%.

2. Pengujian Serangan Terhadap Citra

Perbuatan dari pihak ketiga tidak hanya untuk melihat dan mencuri informasi kada sebuah citra, namun juga bisa untuk membuat penerima citra tidak mengerti apa maksud dari citra yang di dekripsi. Terdapat berbagai serangan yang bisa dilakukan pada citra terenkripsi seperti pemberian *noise*, melakukan *rotation*, proses *filtering*, dan melakukan *cropping* pada citra.

Pengujian dilakukan dengan melakukan serangan pada citra terenkripsi, kemudian dilakukan dekripsi dengan kunci yang sesuai. Dilakukan perhitungan untuk mengetahui perbedaan citra yang terkena serangan dengan citra asli dengan rumus NPCR. Nilai yang diharapkan dari perhitungan NPCR adalah serendah mungkin.

6. Subjek dan Objek Penenlitian

Aplikasi Steganografi ini dirancang dengan menggunakan metode *Discrete Fourier Transform* dengan Bahasa pemrograman C#. Aplikasi ini dikhususkan untuk digunakan pada bidang photography secara khusus digunakan dalam komunitas photography bernama inod photography. Namun juga tidak menutup kemungkinan untuk digunakan leh komunitas photography lainya yang membutuhkan.

7. Alat dan Bahan Penelitian

7.1 Alat Penelitian

1. Perangkat Keras

Spesifikasi kebutuhan perangkat keras yang dibutuhkan untuk menjalankan aplikasi sistem pakar diagnose gannguan kehamilan adalah sebagai berikut :

- *Processor* : Intel core i5 4200U Haswell
- RAM : 4 GB DDR3L
- Graphics : 2GB NVIDIA GeForce GT 740M
- Monitor : 14 inch 1366px x 768px

2. Perangkat Lunak

Spesifikasi kebutuhan perangkat lunak yang dibutuhkan untuk menjalankan aplikasi sistem pakar diagnose gannguan kehamilan adalah sebagai berikut :

- OS Windows 10 Pro
- Microsoft Visual Studio 2012

7.2 Bahan Penelitian

Bahan yang digunakan dalam penelitian adalah beberapa sample foto *full resolution* dari "inod Photography", dan beberapa *watermark* dari "inod Photography". Gambar/foto dan watermark yang digunakan semua dengan format file jpg atau jpeg.

Tabel 3. Contoh Foto yang digunakan

Contoh foto yang akan di digunakan	**Basic info**
	Width : 1184 px Height : 789 px Type file : JPG
	Width : 1184 px Height : 789 px Type file : JPG
	Width : 512 px Height : 512 px Type file : JPG
	Width : 128 px Height : 128 px Type file : JPG

Tabel 4. Contoh Watermark yang digunakan

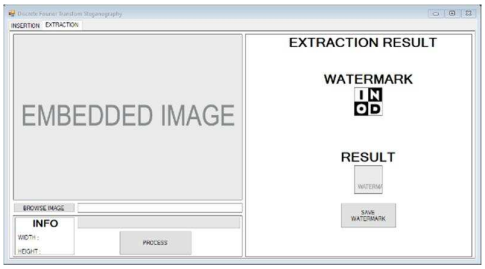
Contoh *watermark* yang di digunakan	Basic info
	Width : 50 px Height : 50 px Type file : JPG

8. Implementasi

Pada tahap impleentasi penulis merancang satutampilan inti yang didalamnya terdapat 2 tab yang masing masing memiliki funsi untuk proses insertion & extraction image. Untuk menjalankanya buka tab insertion dan masukan vessel image atau gambar penampung, & watermark image. Kemudian klik proses untuk menjalankan fungsi memasukkan watermark kedalam vessel image, dan hasil akan muncul pada picturebox kanan. Setelah proses selesai dan hasil terlihat, save image untuk menyimpan hasil gambar atau output dari proses insertion.

Gambar 1. Tab Halaman Insertion

Pada tab extraction untuk menjalnakanya masukan embeded image atau gambar yang telah disisipkan watermark di dalamnya. Kemudian gambar akan diproses dan menghasilkan output berupa watermark yang disisipkan, output akan terlihat pada picture box di sebelah kanan.



Gambar 2. Tab Halaman Extraction

9. Pengujian

Pengujian melalui kesesuaian data dilakukan untuk mengetahui apakah watermark yang berhasil di ekstrak dari citra tersisip sesuai dengan watermark yang disisipkan. Watermark yang digunakan atau disisipkan dapat dilihat pada tabel 5.

Dari data citra penampung dan citra watermark diatas. Selanjutnya lakukan pengujian kesesuaian data dengan menyisipkan watermark kemudian lakukan ekstraksi. Hasil pengujian kesesuaian data ditunjukkan pada Tabel 5.

Tabel 5. Cita Awal, Embeded Image, Dan Watermark Yang Telah Di Ekstraksi Dari Embeded Image.

No	Gambar	*Watermark* Asli	Hasil *Extraction*
1	Picture 1.jpg		
2	Picture 2.jpg		
3	Picture 3.jpg		
4	Picture 4.jpg		

Pada hasil ekstraksi diatas masing-masing citra menghasilkan hasil watermark yang sesuai dengan watermark yang telah disisipkan sebelumnya. Dan pada *embeded image* terlihat idak terdapat perubahan yang signifikan jika dilihat mata.

Pada tabel dibawah dapat dilihat data dari setiap gambar yang telah diuji dengan metode PSNR dan MSE dari Citra awal dan citra tersisip watermark.

Tabel 6. Hasil Perbandingan penyisipan

No	Citra	UACI	NPCR	PSNR
1	Picture 1	0.3780993293 31342	0.9490966796875	27.9304298620428
2	Picture 2	6.50596469056373	15.234375	14.2548977779448
3	Picture 3	0.3632140522 87582	28.316875	32.6551739489079
4	Picture 4	1.5312851307 1895	34.9057291666667	25.6782653216038

Dari tabel diatas dapat disimpulkan bahwa semakin dominan warna hitam pada watermark yang disisipkan kedalam citra semakin rendah nilai PSNR yang didapat. Nilai PSNR terendah ditunjukan pada citra "citra no 2" dengan nilai PSNR 27,8874. Semakin besar dimensi citra yang digunakan maka semakin lama proses penyisipan dan proses ekstraksi watermark. Sehingga untuk mendapatkan hasil ekstraksi yang baik, pada saat melakukan enkripsi sebaiknya watermark yang digunakan dominan berwarna putih.

10. Kesimpulan dan Saran

10. 1 Kesimpulan

Penyisipan *watermark* menggunakan metode *Discrete Fourier Transform* telah dilakukan dengan menggunakan bahasa pemrograman C#. Berdasarkan hasil pengujian yang telah dilakukan, dapat ditarik kesimpulan:

1. *Embeded image* dengan ukuran dimensi citra diatas 512x512 *pixel* memilikit ketahan terhadap serangan *editing* atau *filtering* dibandingkan citra dengan dimensi citra dengan dimensi dibawah 512x512 *pixel.*
2. *Embeded image* tidak tahan terhadap serangan *resize* pembesaran dan pengecilan diatas 10 pixel.
3. *Watermark* akan tidak terbaca jika mendapat serangan *cropping* sebesar 10 *pixel* pada bagian atas *embeded image*
4. Citra dengan ukuran diatas 512x512 *pixel*, memiliki nilai UACI dan NPCR yang kecil dibandingkan dengan citra dengna ukuran dibawah 512x512 *pixel*
5. Pada pengujian PSNR, citra dengan ukuran 512x512 *pixel* memiliki tingkat kemiripan yang lebih banyak jika dibandingkan dengan citra dengan ukuran dibawah 512x512 *pixel*
6. Ukuran citra berpengaruh terhadap kualitas citra penapung.
7. Ukuran dimensi citra berpengaruh terhadap durasi waktu *insertion* & *extraction*.

10.2 Saran

Berdasarkan penelitian yang diperoleh, ada beberapa saran untuk pengembangan sistem lebih lanjut, sebagai berikut:

1. Pengguna dapat memilih watermark sesuai dengan keinginan pengguna.

Daftar Pustaka:

Dhian Sweetania, ST., MMSI, (2015), "*Metode Endkripsi Dekripsi"*. [Online], Tersedia: http://dhian_sweetania.staff.gunadarma.ac.id/ Downloads/files/35348/Enkripsi-I.pdf [26 Desember 2016]

(2013)*, Pengertian citra digital* [Online], Tersedia: http://www.temukanpengertian.com/2013/08/pengertian-citra-digital.html [26 Desember 2016]

(2012), *Pengertian citra digital* [Online], Tersedia : http://repository.usu.ac.id/bitstream/123456789/31325/4/Chapter%20II.pdf [26 Desember 2016]

(2016), *Pengertian Transformasi Fourier Diskrit* [Online], Tersedia: http://www.landasanteori.com/2015/10/pengertian-transformasi-fourier diskrit.html [29 Desember 2016]

(2016), *Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation* (IATFDDFT). [Online], Tersedia: https://arxiv.org/abs/1212.3371 [29 Desember 2016]

(2017), *DFT Based Image Enhancement and Steganography* [Online], Tersedia: static.ijcsce.org/wp-content/uploads/2013/03/IJCSCE020213.pdf [1 Januari 2017]

Rahul, Lokesh, Salony, (2013), *Image Steganography With LSB, International Journal of Advanced Research in Computer Engineering & Technology* (IJARCET), Volume 2, Issue 1, January, [Online], Tersedia: http://www.ijarcet.org/index.php/ijarcet/article/download/675/pdf [5 Maret 2017]